EXHIBIT G

The New York Times Company

Christina M. Koningisor
Legal Department

620 8th Avenue
New York, NY 10018

tel 212-556-1985
christina.koningisor@nytimes.com

February 26, 2018

VIA EMAIL

John Williams
Senior Counselor
Federal Communications Commission
Office of General Counsel
445 12th Street, SW
Washington, DC 20554

Re: New York Times FOIA Appeal – Case No. FCC-2017-764

Dear Mr. Williams,

I write on behalf The New York Times Company and one of its reporters, Nicholas Confessore (together, "The Times") in response to the agency's January 29, 2018 letter supplementing the agency's July 21, 2017 denial of FOIA Request FCC-2017-764. Please consider this a formal appeal of that January 29, 2018 supplemental response. In addition, the Times's appeal of the agency's July 21, 2017 initial response remains pending and is incorporated here by reference.

Procedural History

On June 22, 2017, The Times submitted a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, to the Federal Communications Commission ("the FCC" or "the agency"), for "web server logs for comments submitted for Federal Communications docket No. 17-108 between 4/26/17 and 6/7/17." The request further specified that The Times sought "logs for requests submitted via both to https://www.fcc.gov/ecfs/filings/ and any submissions through the FCC's API (application programming interface)." For each comment, the request sought: (1) Server logs for both GET and POST requests; (2) The date/time stamp of each request; (3) The full query including query strings; (4) The IP address of the client making the request; (5) The browser USERAGENT; and (6) The following headers when available: Accept, Accept-Encoding, Accept-Language, Connection, Host, DNT, Upgrade-Insecure-Requests, Via, X-Forwarded-For."

On July 21, 2017, the FCC denied the request. The FCC stated that the information requested "includes personably [sic] identifiable information and therefore cannot be released." On this basis, the agency withheld the requested records in full. *See* 5 U.S.C. § 552.

On July 25, 2017, The Times appealed the agency's denial. First, the Times argued that Exemption 6 does not apply to the requested records. *See* 5 U.S.C. § 552(b)(6) (shielding from disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy"). Second, The Times argued that even if this exemption did apply, the FCC is obligated to redact or segregate exempt materials rather than withhold the records in full.

The Times and the FCC subsequently engaged in email and telephone communications in an effort to resolve this matter without litigation. In the course of these communications, the FCC raised two additional concerns. First, the agency argued that the requested records would reveal sensitive information about the security measures in place to protect the FCC's notice and comment processes. Second, the agency argued that the request was overly burdensome.

On September 22, 2017, in response to the FCC's security concerns, The Times agreed to narrow its request. It agreed to "[e]liminate all of the following headers: Accept, Accept-Encoding, Accept-Language, Connection, Host, DNT, Upgrade-Insecure-Requests, Via." It requested that the FCC provide the following information: "X-Forwarded-For header, date/time stamp of each request, the fully query including query strings, the IP address of the client making the request, and the browser USERAGENT."

On December 15, 2017, the FCC communicated to The Times via telephone that this narrowed request still did not satisfy the agency's security concerns. On December 19, 2017, the FCC and The Times arranged a phone call in which they discussed a set of parameters that would address the FCC's security concerns. And on December 21, 2017, The Times formally submitted a second proposed narrowing of its request in a further attempt to resolve these concerns. It sought records for comments submitted through both https://www.fcc.gov/ecfs/filings/ and the FCC's API (application programming interface) between April 26, 2017, and June 7, 2017. For each comment on docket number 17-108, it sought the comment, the originating IP address, the date and time stamp, and the User-Agent header.

In its December 21, 2017 letter, The Times also acknowledged that the agency had concerns about the burdensomeness of this narrowed request. It further noted that while it did not have access to the specifics of the architecture used in the agency's ECFS application, it assumed that the agency used a relational database that separates information across several tables and perhaps several databases. As such, The Times proposed that by limiting the request to only four data points, it would thereby limit the number of joins or database lookups required to fulfill the request. The Times also assumed that no manual redactions would be required to respond to this request, as the agency would be able to extract only the information requested, and the agency had previously suggested that these four categories of information would not raise security concerns.

The agency has not responded to The Times's July 25, 2017 appeal. Instead, on January 29, 2018, it submitted a supplemental response to its July 21, 2017 denial of the initial request. In that letter, the agency reiterated its claim that the requested records are exempt from disclosure under FOIA Exemption 6 because they would reveal the commenter's IP address. It then raised two new arguments. First, it argued that the requested server logs may be withheld under FOIA Exemption 7(E) because they would reveal "information about how the Commission protects the security of [the Electronic Comment Filing System] and its other information assets." Second, it argued that "it is not possible to reasonably segregate the exempt from the non-exempt information." The Times now formally appeals this supplemental denial.

Exemption 6

As set out in The Times' July 25, 2017 appeal—incorporated therein by reference—Exemption 6 shields from disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). A two-step analysis determines whether Exemption 6 applies to a particular piece of identifying information. For Exemption 6 to apply: (1) the information must be "contained in 'personnel and medical files and similar files,'" and, if so, (2) the individual privacy interest in non-disclosure of the information must so thoroughly outweigh the public need for the information that "disclosure would constitute a clearly unwarranted invasion of personal privacy." *Assoc. Press v. Dep't of Def.*, 554 F.3d 274, 291 (2d Cir. 2009). The agency's argument that IP addresses may be shielded from disclosure under Exemption 6 fails on both prongs.

First, IP addresses cannot be considered "similar files" within the scope of Exemption 6. The proper analysis for whether a file constitutes a "similar file" under Exemption 6 is to consider the extent of its similarity to the two specific categories of file listed in the exemption: personnel and medical files. *See Dep't of State v. Wash. Post.*, 456 U.S. 595, 600-01 & n.3 (1982). Here, the requested information does not satisfy the threshold test under Exemption 6: it does not reside in a file that is or resembles a personnel or medical file. Instead, it resides in a file containing the information the FCC received from members of the public who voluntarily submit comments as part of its public notice-and-comment rulemaking or other regulatory processes.

Furthermore, companies or individuals that choose to submit a comment to the FCC knowingly and willingly waive whatever privacy interests they might otherwise have had. As The Times's FOIA request observed, the FCC's own comment guide tells prospective commenters:

> Any comments that you submit to the FCC on a proposed rulemaking, petition, or other document for which public comment is requested **will be made public**, including any personally identifiable information you include in your submission. We may share non-personally identifiable information with others, including the public, in aggregated form, in partial or edited form, or verbatim.

See FCC, How to Comment, https://www.fcc.gov/consumers/guides/how-comment (emphasis added). Similarly, the FCC's comment form warns prospective commenters, immediately above the button to proceed to review and file a comment: "You are filing a document into an official FCC proceeding. All information submitted, including names and addresses, **will be publicly**

available via the web." FCC, Submit a Filing, https://www.fcc.gov/ecfs/filings (emphasis added).

Second, releasing a commenter's IP address does not "constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). Exemption 6 is "directed at threats to privacy interests more palpable than mere possibilities." *Dep't of Air Force v. Rose*, 425 U.S. 352, 381 (1976). "To establish that the release of information contained in government files would result in a clearly unwarranted invasion of privacy, the court first asks whether disclosure would compromise a substantial, as opposed to a de minimis, privacy interest." *Nat'l Ass'n of Home Builders v. Norton*, 309 F.3d 26, 33 (D.C. Cir. 2002). If there is a significant privacy interest in the records, "the court then must weigh that interest against the public interest in the release of the records in order to determine whether, on balance, disclosure would work a clearly unwarranted invasion of personal privacy." *Id*. This public interest analysis turns on "the extent to which disclosure would serve the core purposes of the by contributing significantly to public understanding of the operations or activities of the government." *Id*. (internal quotation marks and alteration omitted).

Any privacy interest an individual has in their IP address is de minimis. This is particularly true here, where commenters were participating in an important public debate and were put on notice that "personally identifiable information" included in their submission would be made public. *See* FCC, How to Comment, https://www.fcc.gov/consumers/guides/how-comment. Moreover, the public interest in obtaining these records is substantial. These records reveal the extent to which cloud-based automated bots intervened in an important public debate. In the wake of Special Counsel Robert Mueller's recent indictment of 13 Russian individuals three Russian companies for interfering with U.S. elections and the U.S. political system, the public interest in understanding how these cloud-based automated bots are being used to influence an array of U.S. political activities—including the agency notice and comment process—is exceptionally high.

Exemption 7E

Exemption 7(E) protects "records or information compiled for law enforcement purposes [the production of which] would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk a circumvention of the law." 5 U.S.C. § 552(b)(7)(E).

The agency argues that the requested records would publicly disclose "information about how the Commission protects the security of [the Electronic Comment Filing System] and its other information assets"; "provide detailed information about the Commission's relationship with commercial cloud servers and the infrastructure the Commission uses to manage ECFS and protect it from disruptive attacks"; and "disclose detailed information about the steps the FCC took in response to the spike in ECFS traffic during early May, thereby giving future attackers a 'roadmap' to evade the Commission's future defensive efforts."

This argument is flawed in two respects. First, Exemption 7(E) must be tethered to a law enforcement "investigation[] or prosecution[]." The FCC has not presented any evidence of an

existing or pending investigation or proceeding. Nor does it contend that the FCC itself is involved in any "law enforcement efforts." An agency is not permitted to invoke Exemption 7(E) whenever release of a record might have some harmful effect. Rather, it is narrowly drawn to protect law enforcement techniques, procedures, or guidelines in the context of an investigation or prosecution. *See, e.g.*, *Pinson v. U.S. Dep't of Justice*, 202 F. Supp. 3d 86, 104 (D.D.C. 2016) (rejecting an agency's Exemption 7(E) claim "[b]ecause [the agency] has not shown how the memorandum relates to law enforcement investigations or prosecutions").

Second, The Times has engaged in lengthy discussions with the FCC in an effort to assuage the agency's security concerns. On December 21, 2017, The Times submitted a narrowed request. It was The Times's understanding that this narrowed request would satisfy the agency's security concerns and ensure that neither the agency's "relationship with commercial cloud servers" nor "the steps [it] took" in response to a traffic spike last year would be revealed. The agency's January 29, 2018 letter fails to respond to this narrowing. It does not say whether the agency's security concerns are still valid in the face of The Times's modified request.

Segregability

Finally, the agency argues that nonexempt portions of the request are not "reasonably segregable" from the exempt portions because this information is "inextricably intertwined." It argues that the server logs "consist of hundreds of millions of lines of technical information" and that producing the records would require a line-by-line review by staff personnel.

The Times has limited the scope of its request to four categories of information, none of which are protected from disclosure. It is reasonable to expect that the agency has the technical capacity to extract only those four categories of information, thereby obviating the need for line-by-line review. To the extent that the agency has the capacity, it is obligated to do so. *See Nat'l Sec. Counselors v. C.I.A.*, 898 F. Supp. 2d 233, 270 (D.D.C. 2012). ("Sorting a database by a particular data field (e.g., date, category, title) is essentially 'the application of codes or some form of programming,' and thus does not involve creating new records or conducting research—it is just another form of searching that is within the scope of an agency's duties in responding to FOIA requests.").

Please do not hesitate to contact me with any questions about this appeal. Thank you for your time and assistance.

Sincerely,

Christina Koningisor